AI Security Service

AIセキュリティサービス

最先端の技術と知見を活かした
AIセキュリティサービス

AIシステムの安全性を確保するセキュリティ対策

**AI技術が進化するにつれて、AIシステムには従来のITシステムとは異なる新たな脅威やリスクが発生しており、これに対処するための高度なセキュリティ対策が求められています。
最新の技術に対応したセキュリティ対策を始めてみませんか？**

01 AIセキュリティ教育

当社は、AIやAIシステムの開発者向けに実際の攻撃手法を用いたハンズオン形式のトレーニングを提供し、安全なAI・AIシステム開発のための基礎を構築します。例えば、Pythonなどのコードを用いて実際にAIやAIシステムに対する攻撃をシミュレーションし、その結果から防御策を学ぶ「セキュアAI開発トレーニング」では、攻撃手法の理解を深めると同時に、実際のAIプロジェクトで必要となるセキュリティ対策を実践的に学びます。

02 AIシステムのセキュリティ診断

AIシステムに対するセキュリティ診断サービスでは、擬似的な攻撃を実施して潜在的なリスクを検出し、セキュリティ強化のための対策を提案します。特に、LLMを利用したシステムにおいては、従来のセキュリティ診断では検出が難しいリスクが多く存在します。例えば、LLMがプロンプトインジェクション攻撃を受けることによる機微情報漏えいや、LLMと連携するシステムが攻撃を受ける原因となることがあります。当社は、2015年からAIセキュリティに関する研究を先駆けて行っており、蓄積された知見を基に独自の診断サービスを提供しています。この診断によって、企業はAIシステムに内在するリスクを早期に発見し、迅速に対策を講じることが可能です。

03 AIセキュリティ対策アドバイザリー

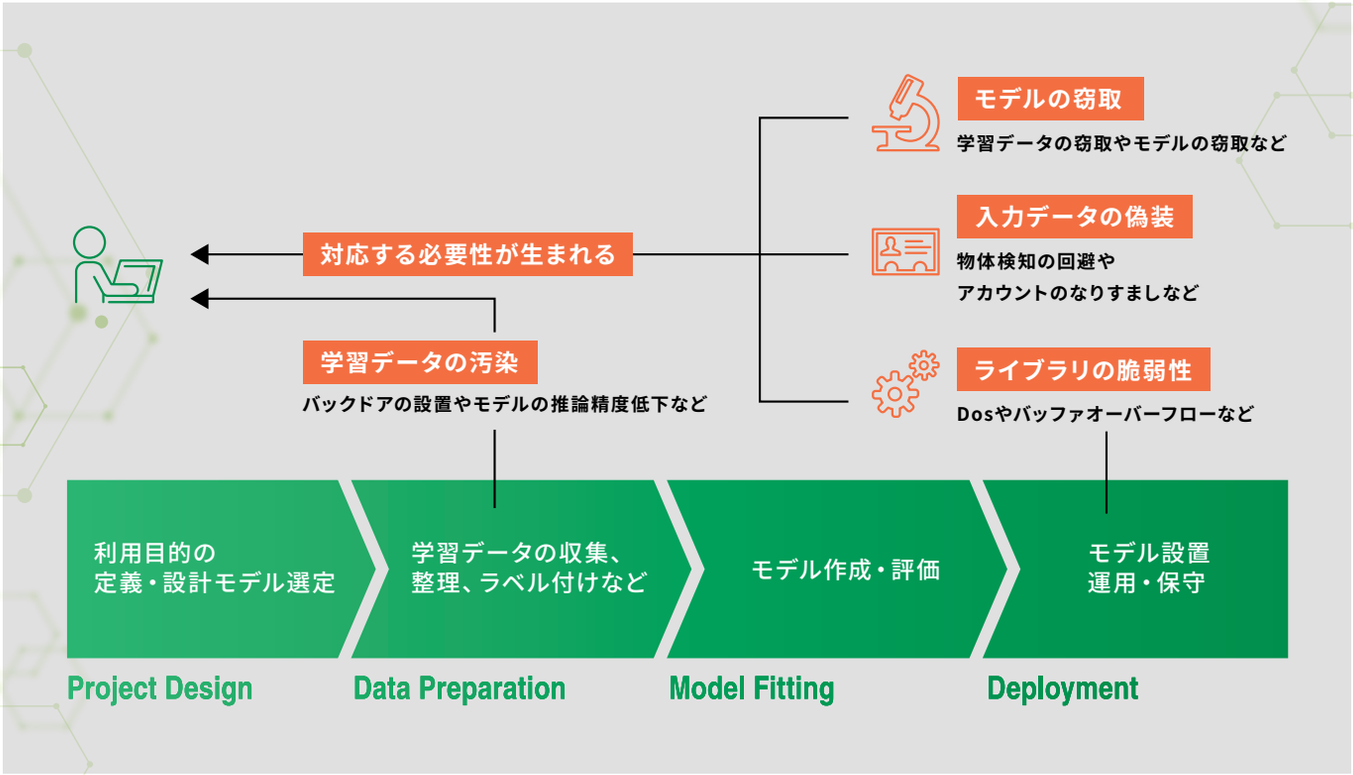
AIシステムの設計段階から導入後の運用まで、あらゆるフェーズでセキュリティ対策を支援するアドバイザリーサービスを提供しています。AIは他のシステムと異なり、特有の脆弱性を持つため、専用の対策が必要です。当社のアドバイザリーサービスでは、技術的なセキュリティ対策に加え、ヒューマンエラーやサプライチェーンリスクにも対応し、ポリシーやガバナンスだけでは防ぎきれないリスクに対しても包括的な支援を行います。これにより、企業はAIシステムの導入や運用に際して、安心してビジネスを推進することができます。

詳しくは裏面へ ⟶

新たな脅威と増大するリスク

大規模言語モデル（LLM）の登場により、新たな脅威が次々と明らかになっています。LLMの利用が拡大する中で、生成された情報が悪用されるリスクが増大しており、例えば「Prompt Leaking」ではAIシステム内部に設定されている機密情報（例：システム・プロンプト）が漏えいする可能性があります。
また、LLMと連携するシステムがSQL Injection攻撃を受ける「P2SQL Injection攻撃」や、LLMを通じて不正なコマンドが実行される「LLM4Shell攻撃」など、最新の技術に対応したセキュリ

▼AI開発の各工程と想定される脅威



生成AI時代における企業のセキュリティリスクと対策の必要性

AIセキュリティは急速に発展している分野であり、日々新たな攻撃手法や防御手法が提案されています。AIは他のシステムとは異なる脅威にさらされるため、従来のセキュリティ対策では十分に対応できないケースも増えています。特に、生成AIの急速な進化に伴い、企業が抱えるリスクはさらに複雑化しています。これに対応するためには、AIセキュリティの専門知識と迅速な対応が求められます。

当社のAIセキュリティサービスは、AI技術の進化とともに発生する最新の脅威に迅速に対応し、お客様のAIシステムを保護するための包括的なソリューションを提供します。これにより、企業はAIシステムの導入や運用に際して、セキュリティリスクを最小限に抑えつつ、安心してビジネスを展開することが可能です。

Information AIセキュリティ紹介ページ **https://www.mbsd.jp/solutions/ai/** お問い合わせ先

その他、情報漏えい調査・セキュリティ監視・セキュリティ対策・セキュリティ診断など、様々な場に応じたセキュリティに関するサービスを扱っております。お気軽にお問い合わせください。

開発元
三井物産セキュアディレクション株式会社
〒103-0013
東京都中央区日本橋人形町1-14-8
JP水天宮前ビル 6階
TEL: 03-5649-1961
Mail: sales-info@mbsd.jp

製品に関する最新情報はこちらから → **www.mbsd.jp**

お問い合わせ

AI11-1003-2510